US5982891:Systems and methods for secure transaction management and electronic rights protection

Inventor(s): **Ginter; Karl L.** , Beltsville, MD
Shear; Victor H. , Bethesda, MD
Spahn; Francis J. , El Cerrito, CA
Van Wie; David M. , Sunnyvale, CA

Applicant(s): **InterTrust Technologies Corp.**, Sunnyvale, CA
News, Profiles, Stocks and More about this company

Issued/Filed Dates: **Nov. 9, 1999** / Nov. 4, 1997

Application Number: **US1997000964333**

IPC Class: **H04L 9/30;**

ECLA Code: **G07F17/16; H04L29/06C6B; H04L29/06; G06F1/00N7R2; G07F7/10F6; H04L29/06C6C2;**

Class: **Current: 705/054;** 705/026; 713/167;
Original: 380/004; 380/024; 380/025; 705/026;

Field of Search: **380/4,25 396/683 705/026 300/024**

Legal Status: Show legal status actions

Abstract: The present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-

electronic information distribution, for example, utilizing the "electronic highway."

Attorney, Agent, or Firm: **Nixon & Vanderhye P.C.;**

Primary/Assistant Examiners: **Barron, Jr.; Gilberto;**

Related Applications:

Application Number	ApplDate	Patent	Issued	Title
US1995000388107	1995-02-13			

Family: Show known family members

U.S. References: Show the 2 patents that reference this one

Patent	Issued	Inventor(s)	Applicant(s)	Title
US3573747	4 /1971	Adams et al.	Institutional Networks Corporation	INSTINET COMMUNICATION SYSTEM FOR EFFECTUATING THE SALE OR EXCHANGE OF FUNGIBLE PROPERTIES BETWEEN SUBSCRIBERS
US3609697	9 /1971	Blevins	International Business Machines Corporation	PROGRAM SECURITY DEVICE
US3796830	3 /1974	Smith	International Business Machines Corporation	RECIRCULATING BLOCK CIPHER CRYPTOGRAPHIC SYSTEM
US3798359	3 /1974	Feistel	International Business Machines Corporation	BLOCK CIPHER CRYPTOGRAPHIC SYSTEM
US3798360	3 /1974	Feistel	International Business Machines Corporation	STEP CODE CIPHERING SYSTEM
US3798605	3 /1974	Feistel	International Business Machines Corporation	CENTRALIZED VERIFICATION SYSTEM
US3806882	4 /1974	Clarke		SECURITY FOR COMPUTER SYSTEMS
US3829833	8 /1974	Freeny, Jr.	Information Identification Company, Inc.	CODE ELEMENT IDENTIFICATION METHOD AND APPARATUS
US3906448	9 /1975	Henriques	RCA Corporation	Fault detection facilitating means for card reader of identification card reading system
US3911397	10 /1975	Freeny, Jr.	Information Identification Inc.	Access control assembly
US3924065	12 /1975	Freeny, Jr.	Information Identification, Inc.	Coherent, fixed BAUD rate FSK communication method and apparatus
US3931504	1 /1976	Jacoby	Basic Computing Arts, Inc.	Electronic data processing security system and method
US3946220	3 /1976	Brobeck et al.	Transactron, Inc.	Point-of-sale system and apparatus
US3956615	5 /1976	Anderson et al.	IBM Corporation	Transaction execution system with secure data storage and

		al.		storage and communications
US3958081	5 /1976	Ehrsam et al.	International Business Machines Corporation	Block cipher system for data security
US3970992	7 /1976	Boothroyd et al.	IBM Corporation	Transaction terminal with unlimited range of functions
US4048619	9 /1977	Forman, Jr. et al.	Digital Data Inc.	Secure two channel SCA broadcasting system
US4071911	1 /1978	Mazur	Continental Can Co. Inc.	Machine control system with machine serializing and safety circuits
US4112421	9 /1978	Freeny, Jr.	Information Identification Company, Inc.	Method and apparatus for automatically monitoring objects
US4120030	10 /1978	Johnstone	Kearney & Trecker Corporation	Computer software security system
US4163280	7 /1979	Mori et al.	Tokyo Shibaura Electric Co., Ltd.	Address management system
US4168396	9 /1979	Best		Microprocessor for executing enciphered programs
US4196310	4 /1980	Forman et al.	Digital Data, Inc.	Secure SCA broadcasting system including subscriber actuated portable receiving terminals
US4200913	4 /1980	Kuhar et al.	International Business Machines Corporation	Operator controlled programmable keyboard apparatus
US4209787	6 /1980	Freeny, Jr.	Gould Inc.	Method for monitoring the location of monitored objects
US4217588	8 /1980	Freeny, Jr.	Information Identification Company, Inc.	Object monitoring method and apparatus
US4220991	9 /1980	Hamano et al.	Tokyo Electric Co., Ltd.	Electronic cash register with removable memory packs for cashier identification
US4232193	11 /1980	Gerard	The Marconi Company Limited	Message signal scrambling apparatus
US4232317	11 /1980	Freeny, Jr.		Quantized hyperbolic and inverse hyperbolic object location system
US4236217	11 /1980	Kennedy		Energy utilization or consumption recording arrangement
US4253157	2 /1981	Kirschner et al.	Alpex Computer Corp.	Data access system wherein subscriber terminals gain access to a data bank by telephone lines
US4262329	4 /1981	Bright et al.	Computation Planning, Inc.	Security system for data processing
US4265371	5 /1981	Desai et al.	Trafalgar Industries Inc.	Foodstuff vending apparatus employing improved solid-state type control apparatus
US4270182	5 /1981	Asija		Automated information input, storage, and

				retrieval system
US4278837	7 /1981	Best		Crypto microprocessor for executing enciphered programs
US4305131	12 /1981	Best		Dialog between TV movies and human viewers
US4306289	12 /1981	Lumley	Western Electric Company, Inc.	Digital computer having code conversion apparatus for an encrypted program
US4309569	1 /1982	Merkle	The Board of Trustees of the Leland Stanford Junior University	Method of providing digital signatures
US4319079	3 /1982	Best		Crypto microprocessor using block cipher
US4323921	4 /1982	Guillou	Etablissement Public de Diffusion dit "Telediffusion de France"	System for transmitting information provided with means for controlling access to the information transmitted
US4328544	5 /1982	Baldwin et al.	International Business Machines Corporation	Electronic point-of-sale system using direct-access storage
US4337483	6 /1982	Guillou	Etablissement Public de Diffusion dit "Telediffusion de France"	Text video-transmission system provided with means for controlling access to the information
US4361877	11 /1982	Dyer et al.	Sangamo Weston, Inc.	Billing recorder with non-volatile solid state memory
US4375579	3 /1983	Davida et al.	Wisconsin Alumni Research Foundation	Database encryption and decryption circuit and method using subkeys
US4433207	2 /1984	Best		Cryptographic decoder for computer programs
US4434464	2 /1984	Suzuki et al.	Hitachi, Ltd.	Memory protection system for effecting alteration of protection information without intervention of control program
US4442486	4 /1984	Mayer	U.S. Philips Corporation	Protected programmable apparatus
US4446519	5 /1984	Thomas	Corban International, Ltd.	Method and apparatus for providing security for computer software
US4454594	6 /1984	Heffron et al.	U.S. Philips Corporation	Method and apparatus to secure proprietary operation of computer equipment
US4458315	7 /1984	Uchenick	Penta, Inc.	Apparatus and method for preventing unauthorized use of computer programs
US4462076	7 /1984	Smith, III	Smith Engineering	Video game cartridge recognition and security system
US4462078	7 /1984	Ross		Computer program protection method
US4465901	8 /1984	Best		Crypto microprocessor that executes enciphered programs
US4471163	9 /1984	Donald et al.		Software protection system
				Method and system for

US4484217	11 /1984	Block et al.	Telease, Inc.	remote reporting, particularly for pay television billing
US4494156	1 /1985	Kadison et al.	Media Systems Technology	Selectable format computer disk copier machine
US4513174	4 /1985	Herman	Standard Microsystems Corporation	Software security method using partial fabrication of proprietary control word decoders and microinstruction memories
US4528588	7 /1985	Lofberg		Method and apparatus for marking the information content of an information carrying signal
US4528643	7 /1985	Freeny, Jr.	FPDC, Inc.	System for reproducing information in material objects at a point of sale location
US4553252	11 /1985	Egendorf		Counting computer software cartridge
US4558176	12 /1985	Arnold et al.		Computer systems to inhibit unauthorized copying, unauthorized usage, and automated cracking of protected software
US4558413	12 /1985	Schmidt et al.	Xerox Corporation	Software version management system
US4562306	12 /1985	Chou et al.		Method and apparatus for protecting computer software utilizing an active coded hardware device
US4562495	12 /1985	Bond et al.	Verbatim Corporation	Multiple system disk
US4577289	3 /1986	Comerford et al.	International Business Machines Corporation	Hardware key-on-disk system for copy-protecting magnetic storage media
US4584641	4 /1986	Guglielmino		Copyprotecting system for software protection
US4588991	5 /1986	Atalla	Atalla Corporation	File access security method and means
US4589064	5 /1986	Chiba et al.	Fujitsu Limited	System for controlling key storage unit which controls access to main storage
US4593353	6 /1986	Pickholtz	Telecommunications Associates, Inc.	Software protection method and apparatus
US4593376	6 /1986	Volk		System for vending program cartridges which have circuitry for inhibiting program usage after preset time interval expires
US4595950	6 /1986	Lofberg		Method and apparatus for marking the information content of an information carrying signal
US4597058	6 /1986	Izumi et al.	Romox, Inc.	Cartridge programming system
US4634807	1 /1987	Chorley et al.	National Research Development Corp.	Software protection device
			International	Implementing a shared higher level of privilege on

US4644493	2 /1987	Chandra et al.	Business Machines Corporation	higher level of privilege on personal computers for copy protection of software
US4646234	2 /1987	Tolman et al.	Brigham Young University	Anti-piracy system using separate storage and alternate execution of selected proprietary and public portions of computer programs
US4652990	3 /1987	Pailen et al.	Remote Systems, Inc.	Protected software access control apparatus and method
US4658093	4 /1987	Hellman		Software distribution system
US4670857	6 /1987	Rackman		Cartridge-controlled system whose use is limited to authorized cartridges
US4672572	6 /1987	Alsberg	Gould Inc.	Protector system for computer access and use
US4677434	6 /1987	Fascenda	Lotus Information Network Corp.	Access control system for transmitting data from a central station to a plurality of receiving stations and method therefor
US4680731	7 /1987	Izumi et al.	Romox Incorporated	Reprogrammable cartridge memory with built-in identification circuitry and programming method
US4683553	7 /1987	Mollier	Cii Honeywell Bull (Societe Anonyme)	Method and device for protecting software delivered to a user by a supplier
US4685056	8 /1987	Barnsdale et al.	Pueblo Technologies, Inc.	Computer security device
US4688169	8 /1987	Joshi		Computer software security system
US4691350	9 /1987	Kleijne et al.	NCR Corporation	Security device for stored sensitive data
US4696034	9 /1987	Wiedemer	Signal Security Technologies	High security pay television system
US4701846	10 /1987	Ikeda et al.	Panafacom Limited	Computer system capable of interruption using special protection code for write interruption region of memory device
US4712238	12 /1987	Gilhousen et al.	M/A-COM Government Systems, Inc.	Selective-subscription descrambling
US4713753	12 /1987	Boebert et al.	Honeywell Inc.	Secure data processing system architecture with format control
US4740890	4 /1988	William	Software Concepts, Inc.	Software protection system with trial period usage code and unlimited use unlocking code both recorded on program storage media
US4747139	5 /1988	Taaffe		Software security method and systems
US4757533	7 /1988	Allen et al.	Computer Security Corporation	Security system for microcomputers

US4757534	7 /1988	Matyas et al.	International Business Machines Corporation	Code protection using cryptography
US4768087	8 /1988	Taub et al.	National Information Utilities Corporation	Education utility
US4791565	12 /1988	Dunham et al.	Effective Security Systems, Inc.	Apparatus for controlling the use of computer software
US4796181	1 /1989	Wiedemer		Billing system for computer software
US4799156	1 /1989	Shavit et al.	Strategic Processing Corporation	Interactive market management system
US4807288	2 /1989	Ugon et al.	C.I.I. Honeywell Bull	Microprocessor intended particularly for executing the calculation algorithms of a public code encoding system
US4817140	3 /1989	Chandra et al.	International Business Machines Corp.	Software protection system using a single-key cryptosystem, a hardware-based authorization system and a secure coprocessor
US4823264	4 /1989	Deming		Electronic funds transfer system
US4827508	5 /1989	Shear	Personal Library Software, Inc.	Database usage metering and protection system and method
US4864494	9 /1989	Kobus, Jr.	Computerized Data Ssytems for Mfg., Inc.	Software usage authorization system with key for decrypting/re-encrypting/re-transmitting moving target security codes from protected software
US4868877	9 /1989	Fischer		Public key/signature cryptosystem with enhanced digital signature certification
US4903296	2 /1990	Chandra et al.	International Business Machines Corporation	Implementing a shared higher level of privilege on personal computers for copy protection of software
US4924378	5 /1990	Hersey et al.	Prime Computer, Inc.	License mangagement system and license storage key
US4930073	5 /1990	Cina, Jr.	International Business Machines Corporation	Method to prevent use of incorrect program version in a computer system
US4949187	8 /1990	Cohen		Video communications system having a remotely controlled central source of video and audio data
US4977594	12 /1990	Shear	Electronic Publishing Resources, Inc.	Database usage metering and protection system and method
US4999806	3 /1991	Chernow et al.		Software distribution system
US5001752	3 /1991	Fischer		Public/key date-time notary facility
				Arrangement with

US5005122	4 /1991	Griffin et al.	Digital Equipment Corporation	cooperating management server node and network service node
US5005200	4 /1991	Fischer		Public key/signature cryptosystem with enhanced digital signature certification
US5010571	4 /1991	Katznelson	Titan Linkabit Corporation	Metering retrieval of encrypted data stored in customer data retrieval terminal
US5023907	6 /1991	Johnson et al.	Apollo Computer, Inc.	Network license server
US5047928	9 /1991	Wiedemer		Billing system for computer software
US5048085	9 /1991	Abraham et al.	International Business Machines Corporation	Transaction system security method and apparatus
US5050213	9 /1991	Shear	Electronic Publishing Resources, Inc.	Database usage metering and protection system and method
US5091966	2 /1992	Bloomberg et al.	Xerox Corporation	Adaptive scaling for decoding spatially periodic self-clocking glyph shape codes
US5103392	4 /1992	Mori	Fujitsu Limited	System for storing history of use of programs including user credit data and having access by the proprietor
US5103476	4 /1992	Waite et al.		Secure system for activating personal computer software at remote locations
US5111390	5 /1992	Ketcham	Unisys Corporation	Software security system for maintaining integrity of compiled object code by restricting users ability to define compilers
US5119493	6 /1992	Janis et al.	International Business Machines Corporation	System for recording at least one selected activity from a selected resource object within a distributed data processing system
US5128525	7 /1992	Stearns et al.	Xerox Corporation	Convolution filtering for decoding self-clocking glyph shape codes
US5136643	8 /1992	Fischer		Public/key date-time notary facility
US5136646	8 /1992	Haber et al.	Bell Communications Research, Inc.	Digital document time-stamping with catenate certificate
US5136647	8 /1992	Haber et al.	Bell Communications Research, Inc.	Method for secure time-stamping of digital documents
US5136716	8 /1992	Harvey et al.	Digital Equipment Corporation	Session control in network for digital data processing system which supports multiple transfer protocols
US5146575	9 /1992	Nolan, Jr.	International Business Machines	Implementing privilege on microprocessor systems for use in software asset

			Corp.	for use in software asset protection
US5148481	9 /1992	Abraham et al.	International Business Machines Corporation	Transaction system security method and apparatus
US5155680	10 /1992	Wiedemer	Signal Security Technologies	Billing system for computing software
US5168147	12 /1992	Bloomberg	Xerox Corporation	Binary image processing for decoding self-clocking glyph shape codes
US5185717	2 /1993	Mori		Tamper resistant module having logical elements arranged in multiple layers on the outer surface of a substrate to protect stored information
US5201046	4 /1993	Goldberg et al.	Xidak, Inc.	Relational database management system and method for storing, retrieving and modifying directed graph data structures
US5201047	4 /1993	Maki et al.	International Business Machines Corporation	Attribute-based classification and retrieval system
US5208748	5 /1993	Flores et al.	Action Technologies, Inc.	Method and apparatus for structuring and managing human communications by explicitly defining the types of communications permitted between participants
US5214702	5 /1993	Fischer		Public key/signature cryptosystem with enhanced digital signature certification
US5216603	6 /1993	Flores et al.	Action Technologies, Inc.	Method and apparatus for structuring and managing human communications by explicitly defining the types of communications permitted between participants
US5221833	6 /1993	Hecht	Xerox Corporation	Methods and means for reducing bit error rates in reading self-clocking glyph codes
US5222134	6 /1993	Waite et al.	Tau Systems Corporation	Secure system for activating personal computer software at remote locations
US5224160	6 /1993	Paulini et al.	Siemens Nixdorf Informationssysteme AG	Process for securing and for checking the integrity of the secured programs
US5224163	6 /1993	Gasser et al.	Digital Equipment Corporation	Method for delegating authorization from one entity to another through the use of session encryption keys
US5235642	8 /1993	Wobber et al.	Digital Equipment Corporation	Access control subsystem and method for distributed computer system using locally cached

			Corporation	locally cached authentication credentials
US5245165	9 /1993	Zhang	Xerox Corporation	Self-clocking glyph code for encoding dual bit digital values robustly
US5247575	9 /1993	Sprague et al.		Information distribution system
US5260999	11 /1993	Wyman	Digital Equipment Corporation	Filters in license management system
US5263158	11 /1993	Janis	International Business Machines Corporation	Method and system for variable authority level user access control in a distributed data processing system having multiple resource manager
US5265164	11 /1993	Matyas et al.	International Business Machines Corporation	Cryptographic facility environment backup/restore and replication in a public key cryptosystem
US5276735	1 /1994	Boebert et al.	Secure Computing Corporation	Data enclave and trusted path system
US5280479	1 /1994	Mary	Matra Communication	Device for insertion of digital packets in a transmission channel
US5285494	2 /1994	Sprecher et al.	PacTel Corporation	Network management system
US5301231	4 /1994	Abraham et al.	International Business Machines Corporation	User defined function facility
US5311591	5 /1994	Fischer		Computer system security method and apparatus for creating and using program authorization information data structures
US5319705	6 /1994	Halter et al.	International Business Machines Corporation	Method and system for multimedia access control enablement
US5337360	8 /1994	Fischer		Method and apparatus for creating, supporting, and using travelling programs
US5341429	8 /1994	Stringer et al.	TestDrive Corporation	Transformation of ephemeral material
US5343527	8 /1994	Moore	International Business Machines Corporation	Hybrid encryption method and system for protecting reusable software components
US5347579	9 /1994	Blandford		Personal computer diary
US5351293	9 /1994	Michener et al.	Wave Systems Corp.	System method and apparatus for authenticating an encrypted signal
US5355474	11 /1994	Thuraisngham et al.		System for multilevel secure database management using a knowledge base with release-based and other security constraints for query, response and update modification
US5373561	12 /1994	Haber et al.	Bell Communications	Method of extending the validity of a cryptographic

			Research, Inc.	certificate
US5390247	2 /1995	Fischer		Method and apparatus for creating, supporting, and using travelling programs
US5390330	2 /1995	Talati		Control system and method for direct execution of software application information models without code generation
US5392220	2 /1995	van den Hamer et al.	U.S. Philips Corporation	Method and system for organizing data
US5392390	2 /1995	Crozier	IntelliLink Corp.	Method for mapping, translating, and dynamically reconciling data between disparate computer platforms
US5394469	2 /1995	Nagel et al.	Infosafe Systems, Inc.	Method and apparatus for retrieving secure information from mass storage media
US5410598	4 /1995	Shear	Electronic Publishing Resources, Inc.	Database usage metering and protection system and method
US5412717	5 /1995	Fischer		Computer system security method and apparatus having program authorization information data structures
US5421006	5 /1995	Jablon	Compaq Computer Corp.	Method and apparatus for assessing integrity of computer system software
US5422953	6 /1995	Fischer		Personal date/time notary device
US5428606	6 /1995	Moskowitz		Digital information commodities exchange
US5438508	8 /1995	Wyman	Digital Equipment Corporation	License document interchange format for license management system
US5442645	8 /1995	Ugon	Bull CP8	Method for checking the integrity of a program or data, and apparatus for implementing this method
US5444779	8 /1995	Daniele	Xerox Corporation	Electronic copyright royalty accounting system using glyphs
US5449895	9 /1995	Hecht et al.	Xerox Corporation	Explicit synchronization for self-clocking glyph codes
US5449896	9 /1995	Hecht et al.	Xerox Corporation	Random access techniques for use with self-clocking glyph codes
US5450493	9 /1995	Maher	AT&T Corp.	Secure communication method and apparatus
US5453601	9 /1995	Rosen	Citibank, N.A.	Electronic-monetary system
US5453605	9 /1995	Hecht et al.	Xerox Corporation	Global addressability for self-clocking glyph codes
US5455407	10 /1995	Rosen	Citibank, N.A.	Electronic-monetary system
US5455861	10 /1995	Faucher et al.	AT&T Corp.	Secure telecommunications

US5455953	11 /1993	Russell	Wang Laboratories, Inc.	Authorization system for obtaining in single step both identification and access rights of client to server directly from encrypted authorization ticket
US5457746	10 /1995	Dolphin	Spyrus, Inc.	System and method for access control for portable data storage media
US5463565	10 /1993	Cookson et al.	Time Warner Entertainment Co., L.P.	Data block format for software carrier and player therefor
US5473687	12 /1995	Lipscomb et al.	Infosafe Systems, Inc.	Method for retrieving secure information from a database
US5473692	12 /1995	Davis	Intel Corporation	Roving software license for a hardware agent
US5479509	12 /1995	Ugon	Bull CP8	Method for signature of an information processing file, and apparatus for implementing it
US5485622	1 /1996	Yamaki	Kabushiki Kaisha Toshiba	Password processing system for computer
US5491800	2 /1996	Goldsmith et al.	Taligent, Inc.	Object-oriented remote procedure call networking system
US5497479	3 /1996	Hornbuckle	SofTel, Inc.	Method and apparatus for remotely controlling and monitoring the use of computer software
US5497491	3 /1996	Mitchell et al.	International Business Machines Corporation	System and method for importing and exporting data between an object oriented computing environment and an external computing environment
US5499298	3 /1996	Narasimhalu et al.	National University of Singapore	Controlled dissemination of digital information
US5504757	9 /1994	Cook et al.	International Business Machines Corporation	Method for selecting transmission speeds for transmitting data packets over a serial bus
US5504837	4 /1996	Griffeth et al.	Bell Communications Research, Inc.	Method for resolving conflicts among distributed entities through the generation of counter proposals by transversing a goal hierarchy with acceptable, unacceptable, and indeterminate nodes
US5508913	4 /1996	Yamamoto et al.	Fujitsu Limited	Electronic automatic offer matching system for freezer exchange transactions among banks
US5509070	4 /1996	Schull	SoftLock Services Inc.	Method for encouraging purchase of executable and non-executable software
US5513261	4 /1996	Maher	AT&T Corp.	Key management scheme for use with electronic

				cards
US5530235	6 /1996	Stefik et al.	Xerox Corporation	Interactive contents revealing storage device
US5530752	6 /1996	Rubin	Convex Computer Corporation	Systems and methods for protecting software from unlicensed copying and use
US5533123	7 /1996	Force et al.	National Semiconductor Corporation	Programmable distributed personal security
US5534975	7 /1996	Stefik et al.	Xerox Corporation	Document processing system utilizing document service cards to provide document processing services
US5537526	7 /1996	Anderson et al.	Taugent, Inc.	Method and apparatus for processing a display document utilizing a system level document framework
US5539735	7 /1996	Moskowitz		Digital information commodities exchange
US5539828	7 /1996	Davis	Intel Corporation	Apparatus and method for providing secured communications
US5550971	8 /1996	Brunner et al.	U S West Technologies, Inc.	Method and system for generating a user interface adaptable to various database management systems
US5553282	9 /1996	Parrish et al.	Taligent, Inc.	Software project history database and method of operation
US5557518	9 /1996	Rosen	Citibank, N.A.	Trusted agents for open electronic commerce
US5568552	10 /1996	Davis	Intel Corporation	Method for providing a roving software license from one node to another node
US5572673	11 /1996	Shurts	Sybase, Inc.	Secure multi-level system for executing stored procedures
US5592549	1 /1997	Nagel et al.	Infosafe Systems, Inc.	Method and apparatus for retrieving selected information from a secure information source
US5613004	3 /1997	Cooperman et al.	The Dice Company	Steganographic method and device
US5621797	4 /1997	Rosen	Citibank, N.A.	Electronic ticket presentation and transfer method
US5629980	5 /1997	Stefik et al.	Xerox Corporation	System for controlling the distribution and use of digital works
US5633932	5 /1997	Davis et al.	Intel Corporation	Apparatus and method for preventing disclosure through user-authentication at a printing node
US5634012	5 /1997	Stefik et al.	Xerox Corporation	System for controlling the distribution and use of digital works having a fee

				digital works having a fee reporting mechanism
US5636292	6 /1997	Rhoads	Digimarc Corporation	Steganography methods employing embedded calibration data
US5638443	6 /1997	Stefik	Xerox Corporation	System for controlling the distribution and use of composite digital works
US5638504	6 /1997	Scott et al.	Object Technology Licensing Corp.	System and method of processing documents with document proxies
US5640546	6 /1997	Gopinath et al.	Network Programs, Inc.	Composition of systems of objects by interlocking coordination, projection, and distribution
US5655077	8 /1997	Jones et al.	Microsoft Corporation	Method and system for authenticating access to heterogeneous computing services
US5687236	11 /1997	Moskowitz et al.	The Dice Company	Steganographic method and device
US5689587	11 /1997	Bender et al.	Massachusetts Institute of Technology	Method and apparatus for data hiding in images
US5692180	11 /1997	Lee	International Business Machines Corporation	Object-oriented cell directory database for a distributed computing environment
US5710834	1 /1998	Rhoads	Digimarc Corporation	Method and apparatus responsive to a code signal conveyed through a graphic image
US5740549	4 /1998	Reilly et al.	PointCast, Inc.	Information and advertising distribution system and method
US5745604	4 /1998	Rhoads	Digimarc Corporation	Identification/authentication system using robust, distributed coding
US5748763	5 /1998	Rhoads	Digimarc Corporation	Image steganography system featuring perceptually adaptive and globally scalable signal embedding
US5748783	5 /1998	Rhoads	Digimarc Corporation	Method and apparatus for robust information coding
US5748960	5 /1998	Fischer		Method and apparatus for validating travelling object-oriented programs with digital signatures
US5754849	5 /1998	Dyer et al.	Wayfarer Communications, Inc.	Self-describing object providing dynamic manipulation of heterogeneous data values and semantic identity between memory and transmission representations
US5757914	5 /1998	McManis	Sun Microsystems, Inc.	System and method for protecting use of dynamically linked executable modules
US5758152	5 /1998	LeTourneau	Prime Arithmetics,	Method and apparatus for the generation and manipulation of data

US5758152	5 /1998	LeTourneau	Inc.	manipulation of data structures
US5765152	1 /1998	Erickson	Trustees of Dartmouth College	System and method for managing copyrighted electronic media
US5768426	6 /1998	Rhoads	Digimarc Corporation	Graphics processing system employing embedded code signals

CLAIMS: [Hide claims]:

We claim:

1. A method for using at least one resource processed in a secure operating environment at a first appliance, said method comprising:

- securely receiving a first entity's control at said first appliance, said first entity being located remotely from said operating environment and said first appliance;
- securely receiving a second entity's control at said first appliance, said second entity being located remotely from said operating environment and said first appliance, said second entity being different from said first entity; and
- securely processing a data item at said first appliance, using at least one resource, including securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item.

2. A method for securely managing at least one operation on a data item performed at least in part by an electronic arrangement disposed at a first site, said method comprising:

- (a) securely delivering a first procedure to said electronic arrangement at said first site from a second site different from said first site;
- (b) securely delivering, to said electronic arrangement at said first site from a third site different from said first and second sites, a second procedure separable or separate from said first procedure; and
- (c) performing, at least in part with said electronic arrangement at said first site, at least one operation on said data item, including using said first and second procedures in combination to at least in part securely manage said operation.

3. A method as in claim 2 including performing said delivering step (b) at a time different from the time said delivering step (a) is performed.

4. A method as in claim 2 wherein said step (a) includes delivering said first procedure from a first source, and said step (b) includes delivering said second procedure from a second source different from said first source.

5. A method as in claim 2 further including ensuring the integrity of said first and second procedures.

6. A method as in claim 2 further including validating each of said first and second procedures.

7. A method as in claim 2 further including authenticating each of said first and second procedures.

8. A method as in claim 2 wherein said using step (c) includes executing at least one of said first and second procedures within a tamper-resistant environment.

9. A method as in claim 2 wherein said step (c) includes the step of controlling said data item with at least one of said first and second procedures.

10. A method as in claim 2 further including establishing a relationship between at least one of said first and second procedures and said data item.
11. A method as in claim 2 further including establishing correspondence between said data item and at least one of said first and second procedures.
12. A method as in claim 2 wherein said delivering step (b) comprises delivering at least one load module encrypted at least in part.
13. A method as in claim 12 wherein said delivering step (a) comprises delivering at least one further load module encrypted at least in part.
14. A method as in claim 2 wherein said delivering step (b) comprises delivering at least one content container carrying at least in part encrypted control information.
15. A method as in claim 2 wherein said delivering step (b) comprises delivering a control method and at least one further method.
16. A method as in claim 2 wherein said delivering step (a) includes:

- encrypting at least a portion of said first procedure,
- communicating said at least in part encrypted first procedure to said electronic arrangement,
- decrypting at least a portion of said first procedure at least in part using said electronic arrangement, and
- validating said first procedure with said electronic arrangement.

17. A method as in claim 2 wherein said delivering step (b) includes delivering at least one of said first and second procedures within an administrative object.
18. A method as in claim 2 wherein said delivering step (b) includes codelivering said second procedure in at least in part encrypted form with said data item.
19. A method as in claim 2 wherein said performing step includes metering usage.
20. A method as in claim 2 wherein said performing step includes auditing usage.
21. A method as in claim 2 wherein said performing step includes budgeting usage.
22. A method of securely controlling use by a third party of at least one protected operation with respect to a data item comprising:

- (a) supplying at least a first control from a first party to said third party;
- (b) supplying, to said third party, at least a second control from a second party different from said first party;
- (c) securely combining. at said third party's location, said first and second controls to form a control arrangement;
- (d) securely requiring use of said control arrangement in order to perform at least one protected operation using said data item; and
- (e) securely performing said at least one protected operation on behalf of said third party with respect to said data item by at least in part employing said control arrangement.

23. A method as in claim 22 wherein said data item is protected.
24. A method as in claim 22 wherein at least one of said plural controls includes a control relating to metering at least one aspect of use of said protected data item.
25. A method as in claim 22 wherein at least one of said plural controls include a control relating to budgeting at least one aspect of use of said protected data item.
26. A secure method for combining data items into a composite

data item comprising:

- (a) securely providing, from a first location to a second location, a first data item having at least a first control associated therewith;
- (b) securely providing, from a third location to said second location, a second data item having at least a second control associated therewith;
- (c) forming, at said second location, a composite of said first and second data items;
- (d) securely combining. at said second location, said first and second controls to form a control arrangement; and
- (e) performing at least one operation on said composite of said first and second data items based at least in part on said control arrangement.

27. A method as in claim 26 wherein said combining step includes preserving each of said first and second controls in said composite set.

28. A method as in claim 26 wherein said performing step comprises governing the operation on said composite of said first and second data items in accordance with said first control and said second control.

29. A method as in claim 26 wherein said providing step includes ensuring the integrity of said association between said first controls and said first data item is maintained during at least one of transmission, storage and processing of said first data item.

30. A method as in claim 26 wherein said providing step comprises delivering said first data item separately from said first control.

31. A method as in claim 26 wherein said providing step comprises codelivering said first data item and said first control.

32. A secure method for controlling a protected operation comprising:

- (a) securely delivering at least a first control and a second control representing rights of first and second entities, respectively, to an electronic appliance used by a third entity; and
- (b) controlling at least one protected operation at least in part in response to a request by said third entity based at least in part on a combination of said first and second controls, including at least one of the following steps:
  - resolving at least one conflict between said first and second controls based on a predefined order;
  - providing an interaction with said third entity to form said combination; and
  - dynamically negotiating between said first and second controls.

33. A method as in claim 32 wherein said controlling step (b) includes controlling decryption of electronic content.

34. A method as in claim 32 further including:

- receiving protected electronic content from a party; and
- authenticating the identity of said party prior to using said received protected electronic content.

35. A method for using at least one resource processed by a secure operating environment, said method comprising:

- securely receiving a first load module provided by a first entity

external to said operating environment;

- securely receiving a second load module provided by a second entity external to said operating environment, said second entity being different from said first entity; and
- securely processing, using at least one resource, a data item associated with said first and second load modules, including securely applying said first and second load modules to manage use of said data item.

36. A secure operating environment system for managing at least one resource comprising:

- a communications arrangement that securely receives a first control of a first entity external to said operating environment, and securely receives a second control of a second entity external to said operating environment, said second entity being different from said first entity; and
- a protected processing environment, operatively connected to said communications arrangement, that:
  - (a) securely processes, using at least one resource, a data item logically associated with said first and second controls, and
  - (b) securely applies said first and second controls to manage said resource for controlling use of said data item.

37. A method as in claim 1 further including securely and persistently associating at least one of said first entity's control and said second entity's control with said data item.

38. A method as in claim 2 further including securely and persistently associating at least one of said first and second procedures with said data item.

39. A method as in claim 22 further including securely and persistently associating at least one of: (a) said first control, (b) said second control, and (c) said control arrangement, with said data item.

40. A method as in claim 26 further including the step of securely ensuring that at least one of (a) said first control, (b) said second control, and (c) said control arrangement, is persistently associated with at least one of said first and second data items.

41. A method as in claim 32 further including the step of persistently and securely associating at least one of said first and second controls with said protected operation.

42. A method as in claim 35 further including the step of persistently and securely associating at least one of said first and second load modules with said data item.

43. A system as in claim 36 wherein said protected processing environment securely and persistently associates at least one of said first and second controls with said data item.

44. A method as in claim 1 further including the step of allowing a user to select between said first entity's control and said second entity's control.

45. A method as in claim 22 further including the step of allowing a user to select between said first procedure and said second procedure.

46. A method as in claim 22 further including the step of allowing a user to select between said first control and said second control.

47. A method as in claim 26 further including the step of allowing a user to select between said first control and said second control.

48. A method as in claim 32 further including the step of allowing a user to select between said first control and said second control.

49. A method as in claim 35 further including the step of allowing a user to select between said first load module and said second load module.

50. A system as in claim 36 wherein said protected processing environment allows said user to select between said first control and

said second control.

51. A method as in claim 1 wherein at least said secure processing step is performed at an end user electronic appliance.

52. A method as in claim 2 wherein at least said performing step is performed at an end user electronic appliance.

53. A method as in claim 22 wherein at least two of the recited steps are performed at an end user electronic appliance.

54. A method as in claim 26 wherein at least one of steps (c), (d) and (e) is performed at an end user electronic appliance.

55. A method as in claim 32 wherein step (b) is performed at an end user electronic appliance.

56. A method as in claim 35 wherein at least two of the recited steps are performed at an end user electronic appliance.

57. A system as in claim 36 wherein said protected processing environment is part of an end user electronic appliance.

58. A method as in claim 1 wherein the step of securely receiving a first entity's control comprises securely receiving said first entity's control from a remote location over a telecommunications link, and the step of securely receiving said second entity's control comprises securely receiving said second entity's control from the same or different remote location over the same or different telecommunications link.

59. A method as in claim 2 wherein step (a) comprises securely delivering said first procedure from a remote location over a telecommunications link, and step (b) comprises securely delivering said second procedure from the same or different remote location over the same or different telecommunications link.

60. A method as in claim 22 wherein step (a) comprises supplying said first control from at least one remote location over a telecommunications link, and step (b) comprises supplying said second control from the same or different remote location over the same or different telecommunications link.

61. A method as in claim 26 wherein step (a) comprises providing said first data item from at least one remote location over a telecommunications link, and step (b) comprises providing said second data item from the same or different remote location over the same or different telecommunications link.

62. A method as in claim 32 wherein step (a) comprises securely delivering said first and second controls from at least one remote location over at least one telecommunications link.

63. A method as in claim 35 wherein said first load module receiving step comprises securely receiving said first load module from at least one remote location over at least one telecommunications link, and said second load module receiving step comprises securely receiving said second load module from the same or different remote location over the same or different telecommunications link.

64. A system as in claim 36 wherein said communications arrangement receives said first and second controls from at least one remote location over at least one telecommunications link.

65. A method as in claim 1 wherein the processing step includes processing said first and second controls within the same secure processing environment.

66. A method as in claim 2 wherein step (c) includes executing said first and second procedures within the same secure processing environment.

67. A method as in claim 22 wherein at least step (c) is performed within the same secure processing environment at said third party's location.

68. A method as in claim 26 wherein step (d) is performed within the same secure processing environment at said second location.

69. A method as in claim 32 wherein step (a) comprises securely delivering said first and second controls into said same secure processing environment used by or on behalf of said third entity.

70. A method as in claim 35 wherein said securely processing step comprises securely executing said first and second load modules within the same secure processing environment.

71. A method as in claim 1 further including the step of securely

combining said first entity's control and said second entity's control to provide a combined control arrangement.

72. A method as in claim 2 further including combining said first and second procedures to provide a combined procedure.

73. A method as in claim 32 further including securely combining said first and second controls to provide a combined control arrangement.

74. A method as in claim 35 further including securely combining said first and second load modules to provide a combined executable.

75. A system as in claim 36 wherein said protected processing environment combines said first and second controls to provide a combined control arrangement.

76. A method as in claim 1 wherein said two securely receiving steps are independently performed at different times.

77. A method as in claim 3 wherein steps (a) and (b) are independently performed.

78. A method as in claim 22 wherein steps (a) and (b) are performed at different times.

79. A method as in claim 26 wherein steps (a) and (b) are performed at different times.

80. A method as in claim 32 wherein step (a) includes securely and independently delivering said first and second controls at different times.

81. A method as in claim 35 wherein said securely receiving steps are performed independently at different times.

82. A system as in claim 36 wherein said communications arrangement independently receives said first and second controls at different times.

83. A method as in claim 2 further including the step (d) of securely conditioning at least one aspect of use of said data item based on said delivering steps (a) and (b) having occurred.

84. A method as in claim 1 wherein at least one of the first entity's control and the second entity's control comprises at least one executable component and at least one data component.

85. A method as in claim 22 wherein at least one of the first and second controls comprises at least one executable component and at least one data component.

86. A method as in claim 26 wherein at least one of the first and second controls comprises at least one executable component and at least one data component.

87. A method as in claim 32 wherein at least one of the first and second controls comprises at least one executable component and at least one data component.

88. A system as in claim 36 wherein at least one of the first control and second controls comprises at least one executable component and at least one data component, and the protected processing environment executes the executable component in a manner that is at least in part responsive to the data component.

89. A method as in claim 1 wherein said first appliance includes a protected processing environment, and wherein:

- said method further comprises a step of receiving, at said first appliance, said data item separately and at a different time from said receiving said first entity's control; and
- said securely processing step is performed at least in part in said protected processing environment.

90. A method as in claim 2 wherein:

- said method further comprises a step of delivering said data item to said electronic arrangement separately and at a different time from said delivering said first procedure; and
- said performing step is performed at least in part in a protected processing environment.

91. A method as in claim 22 wherein:

- said method further comprises supplying said data item to said third party separately and at a different time from supplying of said first control to said third party; and
- said securely performing step comprises performing said protected operation at least in part in a protected processing environment.

92. A method as in claim 26 wherein:

- said method further includes the steps of:
  - providing said first data item separately and at a different time from providing of said first control, and
  - providing said second data item separately and at a different time from providing of said second control; and
- step (e) comprises performing said operation at least in part in a protected processing environment.

93. A method as in claim 32 wherein:

- said method further comprises delivering a data item to said electronic appliance;
- said securely delivering step (a) further comprises delivering at least one of said first control and said second control separately and at a different time from delivering said data item; and
- said method further includes performing said protected operation at least in part in a protected processing environment.

94. A method as in claim 35 wherein said secure operating environment includes a protected processing environment, and wherein:

- said method further comprises receiving a data item within said secure operating environment;
- said first load module receiving step is performed separately and at a time different from receiving said data item; and
- said securely processing step is performed at least in part in said protected processing environment.

95. A secure operating environment system as in claim 36 wherein said communications arrangement also receives a data item separately and at a different time from at least one of said first control and said second control.

96. A method as in claim 1 wherein said first appliance is at least a part of an arrangement at a user site providing an input/output bus connecting a first electronic subsystem with at least a second electronic subsystem, said first electronic subsystem including a first electrical connector connected to said input/output bus, said second electronic subsystem including a second electrical connector connected to said input/output bus, and wherein:

- said method further comprises establishing a secure transmission channel on said input/output bus and transferring at least a portion of said data item over said secure transmission channel from said first electronic to said second electronic subsystem through said first and second

connectors and said input/output bus.

97. A method as in claim 2 wherein said electronic arrangement is disposed at a user site and provides an input/output bus connecting a first electronic appliance with at least a second electronic appliance, said first electronic appliance including a first electrical connector connected to said input/output bus, said second electronic appliance including a further electrical connector connected to said input/output bus, and wherein:

- said method further comprises establishing a secure transmission channel on said input/output bus and transferring at least a portion of said data item over said secure transmission channel from said first electronic appliance to said second electronic appliance through said first and second connectors and said input/output bus.

98. A method as in claim 22 wherein an input/output bus at said third party's location connects a first electronic appliance with at least a second electronic appliance, said first electronic appliance including a first electrical connector connected to said input/output bus, said second electronic appliance including a second electrical connector connected to said input/output bus, and wherein:

- said method further comprises establishing a secure transmission channel on said input/output bus and transferring at least a portion of said data item over said secure transmission channel from first electronic appliance to said second electronic appliance through said first and second connectors and said input/output bus.

99. A method as in claim 26 wherein an input/output bus at said second location connects a first electronic appliance with at least a second electronic appliance, said first electronic appliance including a first electrical connector connected to said input/output bus, said second electronic appliance including a second electrical connector connected to said input/output bus, and wherein:

- said method further comprises establishing a secure transmission channel on said input/output bus and transferring at least a portion of at least one of said first data item and said second data item over said secure transmission channel from first electronic appliance to said second electronic appliance through said first and second connectors and said input/output bus.

100. A method as in claim 32 wherein said electronic appliance includes a first electronic subsystem having a first electrical connector, a second electronic subsystem having a second electronic connector, and an input/output bus connecting said first electronic subsystem with said second electronic subsystem, and wherein:

- said method further comprises establishing a secure transmission channel on said input/output bus and transferring at least a portion of at least one data item over said secure transmission channel from first electronic subsystem to said second electronic subsystem through said first and second connectors and said input/output bus.

101. A method as in claim 35 wherein said secure operating environment is contained within an arrangement at a user site further comprising an input/output bus connecting a first electronic

appliance with at least a second electronic appliance, said first electronic appliance including a first electrical connector connected to said input/output bus, said second electronic appliance including a second electrical connector connected to said input/output bus, and wherein:

- said method further comprises establishing a secure transmission channel on said input/output bus, and transferring at least a portion of said data item over said secure transmission channel from said first electronic appliance to said second electronic appliance through said first and second connectors and said input/output bus.

102. A secure operating environment system as in claim 36 wherein the secure operating environment is located at a user site and wherein:

- said system further comprises:
  - a first electronic appliance including a first electrical connector,
  - a second electronic appliance including a second electrical connector, and
  - an input/output bus connecting said first electrical connector with said second electrical connector; and
- wherein said communications arrangement is coupled to said input/output bus, opens a secure transmission channel on said input/output bus, and transfers at least a portion of said data item over said secure transmission channel through said first and second electrical connectors and said input/output bus.

■

This is a continuation of application Ser. No. 08/388,107, filed Feb. 13, 1995, now abandoned.

■

Background/Summary: Show background/summary

■

Drawing Descriptions: Show drawing descriptions

■

Description of Preferred Embodiments: Show description of preferred embodiments

■

Foreign References:

Publication	Country	Date	IPC Class
BE1984000900479	Belgium	12 /1984	
EP1983000084441	European Patent Office (EPO)	7 /1983	
EP1984000128672	European Patent Office (EPO)	12 /1984	
EP19850A0135422	European Patent Office (EPO)	3 /1985	
EP19900399822A2	European Patent Office (EPO)	11 /1990	
EP19910421409A2	European Patent Office (EPO)	4 /1991	
EP19910456386A2	European Patent Office (EPO)	11 /1991	
EP19920469864A2	European Patent Office (EPO)	2 /1992	
EP19920469864A3	European Patent Office (EPO)	2 /1992	
EP19930565314A2	European Patent Office (EPO)	10 /1993	
EP19940593305A2	European Patent Office (EPO)	4 /1994	

EP19950651554A1	European Patent Office (EPO)	5 /1995	
EP19950668695A2	European Patent Office (EPO)	8 /1995	
EP19960695985A1	European Patent Office (EPO)	2 /1996	
EP19960696798A1	European Patent Office (EPO)	2 /1996	
EP19960715243A1	European Patent Office (EPO)	6 /1996	
EP19960715244A1	European Patent Office (EPO)	6 /1996	
EP19960715245A1	European Patent Office (EPO)	6 /1996	
EP19960715247A1	European Patent Office (EPO)	6 /1996	
EP19960715246A1	European Patent Office (EPO)	6 /1996	
EP19960749081A1	European Patent Office (EPO)	12 /1996	
EP19970778513A2	European Patent Office (EPO)	6 /1997	
EP19970795873A2	European Patent Office (EPO)	9 /1997	
DE1990038039821	Germany	1 /1990	
JP1982000000726	Japan	5 /1982	
JP1987000241061	Japan	10 /1987	
JP1989000068835	Japan	3 /1989	
JP1989000068835	Japan	3 /1989	
JP1990000242352	Japan	9 /1990	
JP1990000247763	Japan	10 /1990	
JP1990000294855	Japan	12 /1990	
JP1992000369068	Japan	12 /1992	
JP1993000181734	Japan	7 /1993	
JP1993000268415	Japan	10 /1993	
JP1993000257783	Japan	10 /1993	
JP1994000001757	Japan	6 /1994	
JP1994000215010	Japan	8 /1994	
JP1994006225059	Japan	8 /1994	
JP1995000084852	Japan	3 /1995	
JP1995000056794	Japan	3 /1995	
JP1995000141138	Japan	6 /1995	
JP1995000200317	Japan	8 /1995	
JP1995007200492	Japan	8 /1995	
JP1995000244639	Japan	9 /1995	
JP1996000137795	Japan	5 /1996	
JP1996000152990	Japan	6 /1996	
JP1996000185298	Japan	7 /1996	
GB1984002136175	United Kingdom	9 /1984	
GB1993002264796	United Kingdom	9 /1993	
WO0001WO0014289	World Intellectual Property Organization (WIPO)	1 /1	
WO1985WOA8502310	World Intellectual Property Organization (WIPO)	5 /1985	

	Organization (WIPO)		
WO1985WO0003584	World Intellectual Property Organization (WIPO)	8 /1985	
WO1990WO0002382	World Intellectual Property Organization (WIPO)	3 /1990	
WO1992WO0022870	World Intellectual Property Organization (WIPO)	12 /1992	
WO1993WO0001550	World Intellectual Property Organization (WIPO)	1 /1993	
WO1994WO0001821	World Intellectual Property Organization (WIPO)	1 /1994	
WO1994WO0003859	World Intellectual Property Organization (WIPO)	2 /1994	
WO1994WO0006103	World Intellectual Property Organization (WIPO)	3 /1994	
WO1994WO0016395	World Intellectual Property Organization (WIPO)	7 /1994	
WO1994WO0018620	World Intellectual Property Organization (WIPO)	8 /1994	
WO1994WO0022266	World Intellectual Property Organization (WIPO)	9 /1994	
WO1994WO0027406	World Intellectual Property Organization (WIPO)	11 /1994	
WO1996WO0000963	World Intellectual Property Organization (WIPO)	1 /1996	
WO1996WO0003835	World Intellectual Property Organization (WIPO)	2 /1996	
WO1996WO0006503	World Intellectual Property Organization (WIPO)	2 /1996	
WO1996WO0005698	World Intellectual Property Organization (WIPO)	2 /1996	
WO1997WO0003423	World Intellectual Property Organization (WIPO)	1 /1997	
WO1997WO0007656	World Intellectual Property Organization (WIPO)	3 /1997	
WO1997WO0032251	World Intellectual Property Organization (WIPO)	9 /1997	
WO1997WO0048203	World Intellectual Property Organization (WIPO)	12 /1997	

Other References:
Article info links by
ISI
THOMSON SCIENTIFIC
:

- IBM Technical Disclosure Bulletin, "Multimedia Mixed Object Envelopes Supporting a Graduated Fee Scheme via Encryption," vol. 37, No. 03, Mar. 1994, Armonk, NY.
- IBM Technical Disclosure Bulletin, "Transformer Rules for Software Distribution Mechanism-Support Products," vol. 37, No. 04B, Apr. 1994, Armonk, NY.
- Suida, Karl, Mapping New Applications Onto New Technologies, "Security Services in Telecommunications Networks," Mar. 8-10, 1988, Zurich.
- Portland Software's ZipLock, Internet information, Copyright Portland Software 1996-1997, 12 pages.
- Stefik, "Internet Dreams: Archetypes, Myths, and Metaphors, Letting Loose the Light: Igniting Commerce in Electronic Publication," pp. 219-253, (1996) Massachusetts Institute of Technology.
- Stefik, Mark, "Letting Loose the Light, Igniting Commerce in Electronic Publication".
- Argent Information Q&A Sheet, http://www.digital-watermark.com/, Copyright 1995, The DICE Company, 7 pages.
- Guillou, L.: "Smart Cards and Conditional Access", pp. 480-490 Advances in Cryptography, Proceedings of EuroCrypt 84 (Beth et al, Ed., Springer-Verlag 1985).

- Struif, Bruno "The Use of Chipcards for Electronic Signatures and Encryption" in: Proceedings for the 1989 Conference on VSLI and Computer Peripherals, IEEE Computer Society Press, 1989, pp. 4/55-4/158.
- Dusse, Stephen R. and Burton S. Kaliski "A Cryptographic Library for the Motorola 56000" in Damgard, I. M., Advances in Cryptology-Proceedings Eurocrypt 90, Springer-Verlag, 1991, pp. 230-244. (15 pages) 16 patents reference this [Article info]
- DSP56000/DSP56001 Digital Signal Processor User's Manual, Motorola, 1990, p. 2-2.
- Rankine, G., "Thomas--A Complete Single-Chip RSA Device," Advances in Cryptography, Proceedings of Crypto 86, pp. 480-487 (A.M. Odlyzko Ed., Springer-Verlag 1987). (8 pages)
- Dyson, Esther, "In tellectual Value," Wired Magazine, Jul. 1995, pp. 136-141 and 182-183 (This article is not prior art.).
- Ryoichi Mori and Masaji Kawahara, The Transactions of the EIEICE, V, "Superdistribution: The Concept and the Architecture," E73 (Jul. 1990), No. 7, Tokyo, Japan.
- "Information Infrastructure Standards Panel: NII `The Information Superhighway`," NationsBank--HGDeal--ASC X9, 15 pages, Date needed.
- Jud Hofmann, "Interfacing the NII to User Homes," Electronic Industries Association, Consumer Electronic Bus Committee, 14 slides, no date, Date needed.
- "Framework for National Information Infrastructure Services," NIST, Jul. 1994, 12 slides.
- Claude Baggett, "Cabel's Emerging Role in the Information Superhighway," Cable Labs, 13 slides, Date needed.
- "IISP Break Out Session Report for Group Number 3, Standards Development and Tracking System," no date, Date needed.
- "XIWT Cross Industry Working Team," 5 pages, Jul. 1994.
- "Computer Systems Policy Project (CSSP), Perspectives on the National Information Infrastructure: Ensuring Interoperability (Feb. 1994)," Feb. 1994.
- "Framework for National Information Infrastructure Services," Draft, U.S. Department of Commerce, Jul. 1994.
- "EIA and TIA White Paper on National Information Infrastructure,"published by the Electronic Industries Association and the Telecommunications Industry Association, Washington, D.C., no date, Date needed.
- Michael Baum, "Worldwide Electronic Commerce: Law, Policy and Controls Conference," program details, Nov. 11, 1993.
- Bruce Sterling, "Literary freeware: Not for Commercial Use," remarks at Computers, Freedom and Privace Conference IV, Chicago, Mar. 26, 1994.
- "The 1:1 Future of the Electronic Marketplace: Return to a Hunting and Gathering Society," 2 pages, no date, Date needed.
- D. Linda Garcia, testimony before a hearing on science, space and technology, May 26, 1994.
- Wired 1.02, "Is Advertising Really dead?, Part 2," 1994.
- Hugh Barnes, memo to Henry LaMuth, subject: George Gilder articles, May 31, 1994.
- Daniel J. Weitzner, A Statement on EFF's Open Platform Campaign as of Nov., 1993, 3 pages.
- "Serving the Community: A Public-Interest Vision of the National Information Infrastructure," Computer Professionals for Social Responsibility, Executive Summary, no date, Date needed.
- Steven Schlossstein, International Economy, "America: The G7's Comeback Kid," Jun./Jul. 1993.
- Lance Rose, "Cyberspace and the Legal Matrix: Laws or Confusion?," 1991.
- Yee, "Using Secure Copressors," CMU-CS-94-149, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA15212, Date needed.
- Tyger et al., "Dyad: A System for Using Physically Secure Coprocessors," School of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213 (undated), Date needed.
- Tygar et al., "Dyad: A System for Using Physically Secure Coprocessors," School of Computer Science, Carnegie Mellon University, Pittsburgh, PA

15213 (May 1991).
- Maxemchuk, "Electronic Document Distribution," AT&T Bell Laboratories, Murry Hill, New Jersey 07974, Date needed.
- Choudhury, et al., "Copyright Protection for Electronic Publishing over Computer Networks," AT&T Bell Laboratories, Murray Hill, New Jersey 07974 (Jun. 1994).
- Weingart, "Physical Security for the μABYSS System," IBM Thomas J. Watson Research Center, Yorktown Heights, New York 10598 (1987).
- White, "ABYSS: A Trusted Architecture for Software Protection," IBM Thomas J. Watson Research Center, Yorktown Heights, New York 10598 (1987).
- Neumann, et al., "A Provably Secure Operating System: The System, Its Applications, and Proofs," Computer Science Laboratory Report CSL-116, Second Edition, SRI International (May 1980).
- Caruso, "Technology, Digital Commerce 2 plans for watermakrs, which can bind proof of authorship to electronic works," New York Times (Aug. 1995).
- "Electronic Currency Requirements, XIWT (Cross Industry Working Group)," no date, Date needed.
- "NII, Architecture Requirements, XIWT," no date, Date needed.
- Arthur K. Reilly, Standards committee T1-Telecommunications, Input to the `International Telecommunications Hearings,` Panel 1: Component Technologies of the NII/GII, no date, Date needed.
- Dan Bart, Comments in the Matter of Public Hearing and Request for Comments on the International Aspects of the National Information Infrastructure, Aug. 12, 1994.
- "Open System Environment Architectural Framework for National Information Infrastructure Services and Standards, in Support of National Class Distributed Systems," Distributed System Engineering Program Sponsor Group, Draft 1.0, Aug. 5, 1994.
- "Cable Television and America's Telecommunications Infrastructure," National Cable Television Association, Apr. 1993.
- Adele Weder, "Life on the Infohighway," 4 pages, no date, Date needed.
- T. Valovic, Telecommunications, "The Role of Computer Networking in the Emerging Virtual Marketplace," pp. 40-44, Date needed.
- Dr. Joseph N. Pelton, Telecommunications, "Why Nicholas Negroponte is Wrong About the Future of Telecommunication," pp. 35-40, Jan. 1993.
- Nicholas Negroponte, Telecommunications, "Some Thoughts on Likely and expected Communications scenarios: A Rebuttal," pp. 41-42, Jan. 1993.
- Tom Stephenson, Advanced Imaging, "The Info Infrastructure Initiative: Data SuperHighways and You," pp. 73-74, May 1993.
- Steve Rosenthal, New Media, "Mega Channels," pp. 36-46, Sep. 1993.
- News Release, The White House, Office of the President, "Background on the Administration's Telecommunications Policy Reform Initiative," Jan. 11, 1994.
- Steve Rosenthal, New Media, "Interactive Network: Viewers Get Involved," pp. 30-31, Dec. 1992.
- Steve Rosenthal, New Media, "Interactive TV: The Gold Rush Is On," pp. 27-29, Dec. 1992.
- EFFector Online vol. 6 No. 6, "A Publication of the Electronic Frontier Foundation," 8 pages, Dec. 6, 1993.
- Mike Lanza, electronic mail, "George Gilder's Fifth Article--Digital Darkhorse--Newspapers," Feb. 21, 1994.
- Steven Levy, Wired, "E-Money, That's What I Want," 10 pages, Dec. 1994.
- Kevin Kelly, Whole Earth Review, "E-Money,"pp. 40-59, Summer 1993.
- Green paper, "Intellectual Property and the National Information Infrastructure, a Preliminary Draft of the Report of the Working Group on Intellectual Property Rights," Jul. 1994.
- Communications of the ACM, "Intelligent Agents," Jul. 1994, vol. 37, No. 7.
- "Encapsulation: An Approach to Operating System Security," Bisbey, II et al., Oct. 1973, pp. 666-675.
- "Encryption Methods in Data Networks," Blom et al., Ericsson Technics, No. 2, 1978, Stockholm, Sweden.
- First CII Honeywell Bull International Symposium on Computer Security and

Confidentiality, Jan. 26-28, 1981, Conference Text, pp. 1-21.
- Codercard, Spec Sheet--Basic Coder Subsystem, No date given, Date needed.
- "Micro Card"--Micro Card Technologies, Inc., Dallas, Texas, No date given, Date needed.
- "A Method of Software Protection Based on the Use of Smart Cards and Cryptographic Techniques," Schaumueller-Bichl et al., No date given, Date needed.
- I "The New Alexandria" No. 1, Alexandria Institute, pp. 1-12, Jul.-Aug. 1986.
- Denning et al., "Data Security," 11 Computing Surveys No. 3, Sep. 1979.
- Kent, "Protecting Externally Supplied Software In Small Computers" (MIT/LCS/TR-255 Sep. 1980).
- Proceedings of the IEEE, vol. 67, No. 3, Mar. 1979, "Privacy and Authentication: An Introduction to Cryptography," Whitfield Diffie and Martin E. Hellman, pp. 397-427. (31 pages)
- Digest of Papers, VLSI: New Architectural Horizons, Feb. 1980, "Preventing Software Piracy With Crypto-Microprocessors," Robert M. Best, pp. 466-469.
- IEEE Transactions on Information Theory, vol. 22, No. 6, Nov. 1976, "New Directions in Cryptography," Whitfield Diffie and Martin E. Hellman, pp. 644-651. (11 pages)
- Low, et al., "Anonymous Credit Cards," AT&T Bell Laboratories, Proceedings of the 2nd ACM Conference on Computer and Communication Security, Fairfax, Virgina, Nov. 2-4, 1994.
- Tygar et al., "Cryptography: It's Not Just For Electronic Mail Anymore," CMU-CS-93-107, School of Computer Science Carnegie Mellon University, Pittsburgh, Pennsylvania, Mar. 1, 1993.
- Smith, et al., "Signed Vector Timestamps: A Secure Protocol for Partial Order Time," CMU-93-116, School of Computer Science Carnegie Mellon University, Pittsburgh, Pennsylvania, Oct. 1991; version of Feb. 1993.
- Kristol et al., "Anonymous Internet Mercantile Protocol," AT&T Bell Laboratories, Murray Hill, New Jersey, Draft: Mar. 17, 1994.
- Low et al., "Document Marking and Identification using both Line and Word Shifting," AT&T Bell Laboratories, Murray Hill, New Jersey, Jul. 29, 1994.
- Low et al., "Anonymous Credit Cards and its Collusion Analysis," AT&T Bell Laboratories, Murray Hill, New Jersey, Oct. 10, 1994.
- "Applications Requirements for Innovative Video Programming; How to Foster (or Cripple) Program Development Opportunities for Interactive Video Programs Delivered on Optical Media; A Challenge for the Introduction of DVD (Digital Video Disc)" (Oct. 19-20, 1995, Sheraton Universal Hotel, Universal City CA).
- Bruner, Rick E., "PowerAgent, NetBot help advertisers reach Internet shoppers," Aug. 1997 (Document from Internet).
- CD ROM, "Introducing . . . The Workflow CD-ROM Sampler," Creative Networks, MCIMail: Creative Networks, Inc., Palo Alto, California.
- Clark, Tim, "Ad service gives cash back," www.news.com, Aug. 4, 1997, 2 pages (Document from Internet).
- Dempsey, et al., D-Lib Magazine, Jul./Aug. 1996 "The Warwick Metadata Workshop: A Framework for the Deployent of Resource Description," Jul. 15, 1966.
- Firefly Network, Inc., www.ffly.com, "What is Firefly?" Firefly revision: 41.4 Copyright 1995, 1996.
- Harman, Harry H., Modern Factor Analysis, Third Edition Revised, University of Chicago Press Chicago and London, Third revision published 1976.
- Herzbert, Amir et al., "Public Protection of Software," ACM Transactions on Computer Systems, vol. 5, No. 4, Nov. 1987, pp. 371-393. (23 pages)
- Holt, Stannie, "Start-up promises user confidentiality in Web marketing service," Info World Electric, Aug. 13, 1997 (Document from Internet).
- Jiang, et al., "A concept-Based Approach to Retrieval from an Electronic Industrialn Directory," International Journal of Electronic Commerce, vol. 1, No. 1, Fall 1996, pp. 51-72.
- Jones, Debra, "Top Tech Stories, PowerAgent Introducts First Internet `Infomediary` to Empower and Protect Consumers," Aug. 13, 1997 3 pages (Document from Internet).

- Lagoze, Carl, D-Lib Magazine, Jul./Aug. 1996, "The Warwick Framework, A Container Architecture for Diverse Sets of Metadata,".
- Maclachlan, Malcolm, "PowerAgent Debuts Spam-Free Marketing," TechWire, Aug. 13, 1997, 3 pages (Document from Internet).
- Mossberg, Walter S., "Personal Technology, Threats to Privacy On-Line Become More Worrisome," Wall Street Journal, Oct. 24, 1996.
- Negroponte, "Electronic Word of Mouth," Wired Oct. 1996, p. 218.
- PowerAgent Inc., "Power Use of Consumer Information on the Internet White Paper," Jun. 1997, Document from Internet, 9 pages (Document from Internet).
- PowerAgent Press Releases, "What the Experts are Reporting on PowerAgent," Aug. 13, 1997, 6 pages (Document from Internet).
- PowerAgent Press Releases, "What the Experts are Reporting on PowerAgent," Aug. 4, 1997, 5 pages (Document from Internet).
- PowerAgent Press Releases, "What the Experts are Reporting on PowerAgent," Aug. 13, 1997, 3 pages (Document from Internet).
- Resnick, et al., "Recommender Systems," Communications of the ACM, vol. 40, No. 3, Mar. 1997,pp. 54-89.
- Rothstein, Edward, The New York Times, "Technology, Connections, Making th eInternet come to you, through `push` technology.". pp D5, Jan. 20, 1997.
- Rutkowski, Ken, PowerAgent Introduces First Internet `Infomediary` to Empower and Protect Consumers, Tech Talk News Story, Aug. 4, 1997 (Document from Internet).
- Sager, Ira (Edited by), "Bits & Bytes", Business Week, Sep. 23, 1996, p. 142E.
- Schurmann, Jurgen, Pattern Classification, A Unified View of Statistical and Neural Approaches, John Wiley & Sons, Inc., 1996.
- Special Report, "The Internet:Fulfilling the Promise" "The Internet: Bring Order From Chaos"; Lynch, Clifford, "Search the Internet"; Resnick, Paul, "Filtering Information on the Internet"; Hearst, Marti A., "Interfaces for Searching the Web"; Stefik, Mark, "Trusted Systems"; Scientific American, Mar. 1997, pp. 49-56, 62-64, 68-72, 78-81.
- Stefik, Mark, Introduction to Knowledge Systems, Chapter 7, "Classification," pp. 543-607, 1995 by Morgan Kaufmann Publishers, Inc.
- Voight, Joan, "Beyond the Banner," Wired, Dec. 1996, pp. 196, 200, 204.
- Vonder Haar, Steven, "PowerAgent Launches Commercial Service," Inter@ctive Week, Aug. 4, 1997 (Document from Internet).
- Shear, "Solutions for CD-ROM Pricing and Data Security Problems", pp. 530-533, CD ROM Yearbook 1988-1989 (Microsoft Press 1988 or 1989).
- Press Release, "National Semiconductor and EPR Partner For Information Metering/Data Security Cards" (Mar. 4, 1994).
- "Electronic Publishing Resources Inc. Protecting Electronically Published Properties Increasing Publishing Profits" (Electronic Publishing Resources 1991).
- "The Benefits of ROI For Database Protection and Usage Based Billing" (Personal Library Software, 1987 or 1988).
- DiscStore (Electronic Publishing Resources 1991).
- ROI (Personal Library Software, 1987 or 1988).
- ROI-Solving Critical Electronic Publishing Problems (Personal Library Software, 1987 or 1988).
- Collection of documents including "Protecting Electronically Published Properties, Increasing Publishing Profits," (25 pages), Electronic Publishing Resources Inc., Jan. 1993.
- Weber, "Metering Technologies for Digital Intellectual Property, A Report to the International Federation of Reproduction Rights Organisations," pp. 1-29; Oct. 1994 Boston, MA, USA.
- World Wide Web FAO, "How can I put an access counter on my home page?," 1 page (1996).
- Document from Internet, cgi@ncsa.uiuc.edu, "CGI Common Gateway Interface," 1 page (1996).
- Document from Internet, java@java.sun.com, "JAVA Soft, Frequently Asked Questions--Applet Security," 8 pages (Jun. 7, 1996).

- Document from Internet, "HotJava(tm): The Security Story," 4 pages (undated).
- Document from Internet, "Low Level Security in Java," Frank Yellin, 8 pages (Sun Microsystems 1996).
- Document from Internet, "Digital Rights Management Technologies," Robert Weber, 21 pages (Oct. 1995).
- Weber, Robert, "Digital Rights Management Technologies, A Report to the International Federation of Reproduction Rights Organisations," Northeast Consulting Resources, Inc., 49 pages (Oct. 1995).
- Document from Internet, "Softic Symposium '95, Copyright Clearances and Moral Rights," Fred Greguras, 3 pages (Dec. 11, 1995).
- "Invoice? What's an Invoice?"; Business Week (Jun. 10, 1996).
- Communications of the ACM, vol. 39, No. 6 (Jun. 1996).
- Templar Overview, 4 pages (undated, Premenos).
- Document from Internet, "A Supplement to Midrange Systems, Premenos Corp. What Papter: The Future of Electronic Commerce," 4 pages (Premenos, after Aug. 1995).
- Document from Internet, info@templar.net, "Templar Software and Services, Secure, Reliable, Standards-Based EDI Over the Internet," 1 page (Premenos, undated).
- Document from Internet, "Premenos Announces Templar 2.0--Next Generation Software for Secure Internet EDI," 1 page (Feb. 17, 1996).
- Document from Internet, "News from The Document Company Xerox, Xerox Announces Software Kit For Creating `Working Documents` with Dataglyphs" 13 pages (Nov. 6, 1995).
- Document from Internet, info@surety.com, "About the Digital Notary Service," 1994-5, 6 pages (Surety Technologies 1995).
- Document from Internet, Barassi, Theodore Sedgwick, "The Cybernotary: Public Key Registration and Certification and Authentication of International Legal Transactions," 4 pages (undated).
- AT&T Technology, vol. 9, No. 4, "New Products, Systems and Services," pp. 16-19 (undated).
- Document from Internet, News Release, "AT&T encryption system protects information services," 1 page (Jan. 9, 1995).
- Document from Internet, News Release, "AT&T, VLSI Technology join to improve info highway security," 3 pages (Jan. 31, 1995).
- Document form Internet, "Steganography Info and Archive," 2 pages (Eric Milbrandt 1996).
- Document from Internet, "WEPIN Store, Steganography (Hidden Writing)," 1 page (Commun Law 1995).
- Document from Internet, marit@schulung.netuse.de, "Sag's durch die Blume," 5 pages (German, undated).